REMARKS

Claims 1-19 were presented for examination and were rejected. Reconsideration of this application, as amended by the Examiner's Amendment mailed October 6, 2005, and allowance of all claims herein, claims 1-19 as originally presented, are hereby respectfully requested.

On page 2 of his Office Action, the Examiner stated that on May 4, 2007, Applicants filed an IDS listing three items, one of which is a DVD (United States Air Force Audio Visual Presentation), and that there were 20 other documents filed as exhibits without explanation and unlisted on any 1449 form. The Examiner requested that Applicants provide information to explain the nature of these exhibits, to identify the litigation (if any) relating to these items, and to identify their relation to the present patent application.

Applicants submitted a written transcript of the DVD with their IDS mailed August 2, 2007.

The 20 documents were submitted to the USPTO as part of exhibits to reference 2L with the IDS filed on May 4, 2007. As stated in said IDS, reference 2L is a pleading (Defendant Visa International Service Association's Final Invalidity Contentions for U.S. Patent No. 6,327,661 pursuant to Patent Local Rule 3-6(B), filed in the lawsuit Cryptography Research, Inc. v. Visa International Service Association, United States District Court Case No. 5:04-CV--04143-JW (HRL), Northern District of California, San Jose Division, December 8, 2006). The patent involved in said litigation is related to the subject matter of the present patent application.

In view of the above observations, Applicants hereby request the Examiner to consider all three references that they submitted to the USPTO as part of said IDS filed May 4, 2007.

The Examiner rejected claims 1-19 under 35 U.S.C. § 102(e) as being anticipated by Gressel et al., U.S. patent 6,748,410. The rejected claims constitute all of the claims of the

present patent application. Out of these claims, claims 1, 2, 3, 12, and 18 are independent, and the other claims are dependent.

Applicants respectfully traverse this rejection, for the reasons enumerated below.

1. THE CITED PORTIONS OF GRESSEL DO NOT QUALIFY UNDER 35 U.S.C. §102(e)

Under §102(e), the alleged prior art must have an effective filing date prior to the effective filing date of the application against which it is applied.

Gressel is a CIP of U.S. patent application 09/050,958 (now issued as U.S. patent 6,185,596) to Hadad. Hadad was filed on April 1, 1998. The new matter in Gressel over Hadad was filed on January 10, 2000.

The present application is a combination of three earlier parent patent application families. The present application claims priority upon, inter alia:

U.S. patent application 09/326,222 filed on June 3, 1999;

U.S. patent application 09/324,798 filed on June 3, 1999; and

U.S. patent application 09/224,682 filed on Dec. 31, 1998.

The present claims are supported by the specifications of these three parent applications. Thus, the present application has an effective filing date at least as early as the latest of these three parent applications, namely, June 3, 1999.

Therefore, in order for the cited portions of Gressel to qualify under §102(e) against the present application, the portions of Gressel must have been found in Gressel's parent (Hadad, filed on April 1, 1998). That is, any matter added in Gressel as part of the CIP filing date (January 10, 2000) cannot qualify as a §102(e) reference.

A comparison of the specifications of Gressel and Hadad shows clearly which portions of Gressel were originally in Hadad, and which were added as part of the CIP:

Gressel Specification Section	Gressel Specification References	Hadad Specification Section	Hadad Specification References	Does this portion of Gressel qualify under 102(e)?
FIGS. 1-5		FIGS. 1-5		YES
FIGS. 6A-16		**MISSING**		**NO**
Summary	col. 1, line 38 – col. 9, line 39	Summary	col. 1, line 21 – col. 9, line 25	YES
Summary	**col. 9, line 40 – col. 27, line 20**	**MISSING**	**MISSING**	**NO**
Brief Description of Drawings	col. 27, line 21 – col. 29, line 44	Brief Description of Drawings	col. 9, line 26 – col. 9, line 50	YES
Brief Description of Drawings	**col. 27, line 45 – col. 29, line 25**	**MISSING**	**MISSING**	**NO**
Description of Preferred Embodiment	col. 29, line 26 – col. 39, line 59	Description of Preferred Embodiment	col. 9, line 51 – col. 20, line 17	YES
Description of Preferred Embodiment	**col. 39, line 60 – col. 62, line 2**	**MISSING**	**MISSING**	**NO**
Concluding boilerplate	col. 62, line 3 – col. 62, line 26	Concluding boilerplate	col. 20, line 18 – col. 20, line 41	YES

That is, the following portions of Gressel do not qualify under §102(e) against the present application:

col. 9, line 40 – col. 27, line 20;

col. 27, line 45 – col. 29, line 25; and

col. 39, line 60 – col. 62, line 2

(collectively, the "**Non-102(e) Portions of Gressel**").

However, the Office Action shows that the Non-102(e) Portions of Gressel are relied on[1] for every element of independent claims 1, 2, 3, 12, and 18. For this reason alone, Applicants respectfully assert that the §102(e) rejection is improper.

2. THE CITED PORTIONS OF GRESSEL APPEAR TO REFLECT APPLICANTS' OWN INVENTIONS

Even ignoring Gressel's date problems with respect to §102(e), there is yet a second reason why Gressel is not a proper §102(e) reference. §102(e) requires that the portions of the reference being asserted must have been invented "by another" (i.e., someone other than the Applicants).

In that regard, Applicants respectfully point out that at least some of the cited portions of Gressel are simply an acknowledgement of Applicants' own work. For example, Gressel, col. 21, lines 15-35 (cited against independent claim elements 1(a), 1(d), and corresponding elements of the other independent claims) refer to a Web document authored by Paul Kocher, Joshua Jaffe, and Benjamin Jun -- who are the very inventors on the present application. Clearly, these portions of Gressel cannot qualify under §102(e).[2]

This is hardly surprising, given that Paul Kocher and his team are widely acknowledged as the discoverer of so-called differential power analysis ("DPA") attacks against cryptographic systems, as well as countermeasures against such attacks.[3] For example, see the attached article from the New York Times, attached hereto as Appendix A.

---

[1] Either per se or, in a very small minority of cases, in combination with other portions of Gressel that may qualify under §102(e), namely, claim elements 1(a) [col. 1, lines 47-54; col. 3, lines 14-19; and col. 1, lines 61-65] and 18(h) [col. 8, lines 45-50].

[2] Applicants have not done a comprehensive analysis of the other cited portions of Gressel, since the single example cited above is sufficient to traverse.

[3] The three parent utility applications (referred to above) upon which the present application is based include claims on the countermeasures, and the present application includes claims on the attack.

Since at least some of the relied-upon disclosures from Gressel are in fact references to the Applicants' own work, this is yet an additional reason that the §102(e) rejection is improper.

3. THE CITED PORTIONS OF GRESSEL ARE INCONSISTENT WITH EACH OTHER, AND DO NOT SATISFY THE RELATIONSHIP REQUIRED BY THE CLAIMS

Even ignoring Gressel's date and inventorship problems with respect to §102(e), there are still more (technical) reasons why the claims in the present application are novel and non-obvious over Gressel.

As just one example, claim 1 (and other corresponding independent claims) require connecting a device to a "digital-to-analog converter" in 1(a) and taking power measurements using "said analog-to-digital converter" in 1(c). That is, the analog-to-digital converter in 1(a) should correspond to the one used in 1(c).

In the Office Action, the analog-to-digital converter cited for 1(a) (Gressel, col. 50, lines 58-64) is used to implement countermeasures within the device. In contrast, the analog-to-digital converter cited for 1(c) (Gressel, col. 21, lines 29-35 – again, a reference to Paul Kocher's early work on the subject) is used to take measurements external to the device.

Since the cited portions of Gressel are inconsistent with each other, and do not satisfy the relationship required by the claims, this is yet another reason why the rejection over Gressel is improper.

CONCLUSION

For at least the three reasons given above, Applicants respectfully submit that the cited portions of Gressel are not a proper §102(e) reference with respect to the pending application, and that the pending claims are clearly distinguished over Gressel. Accordingly, Applicants request that the pending application be passed to allowance.

Applicants believe that this application is in condition for allowance of all claims herein, claims 1-19 as originally presented, and therefore an early Notice of Allowance is respectfully requested. If the Examiner disagrees or believes that, for any other reason, direct contact with Applicants' attorney would help advance the prosecution of this case to finality, he is invited to telephone the undersigned at the number given below.

Respectfully submitted,

date of signature: April 4, 2008

Edward J. Radlo
Attorney of Record
Reg. No. 26,793

SONNENSCHEIN NATH & ROSENTHAL LLP
P. O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(415) 882-2402

attachment and enclosures

cc: IP/T docket CH (w/attach. & encl.)
J. Yang (") DPA-OMNI (DPAWS)

June 22, 1998

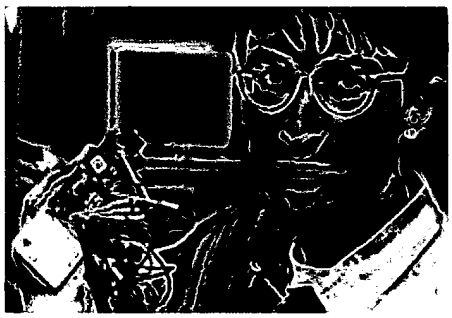
Code Breaker Cracks Smart Cards' Digital Safe

By PETER WAYNER

To the companies in the smart card business, Paul Kocher may be too smart for their own good.

For the last year, Kocher's four-man consulting firm in San Francisco has kept big credit card companies and banks on edge by sharing details of his discovery of a way to break into the newest version of smart cards -- credit-card size devices that contain a tiny computer chip and can be used for a variety of purposes including storing so-called digital cash.

Although Kocher's intent has been to warn the industry and sell it possible solutions, his expertise, in the hands of thieves, counterfeiters or impostors, could compromise the security safeguards of smart cards, which are coming into widespread use in this country and in Europe.



Credit: Peter DaSilva for The New York Times

Paul Kocher of Cryptography Research holds a modified "smart card" reader he developed to help decipher the digital code of the cards that are used by banks and financial institutions.

The cards are at the center of the plans by the banking and credit card industries to cut costs and improve customer convenience by replacing conventional magnetic-stripe cards with ones that not only can act as a debit or automated-teller-machine card but can also be loaded with digital cash that would function as legal tender wherever merchants have digital-cash decoder terminals.

Public confidence in the technology will be crucial to the industry's plans. And that may help explain why, since word leaked of Kocher's break-in methods two weeks ago, the industries promoting smart cards have tended to play down his technique by calling it a "laboratory attack" that could be replicated by perhaps a handful of people around the world.

"Chip cards are the most secure technology around," said Steve Schapp, the executive vice president of Visa International in charge of developing smart cards. "They are very hard to break."

Kocher and his colleagues were able to crack the digital code designed to make

APPENDIX A
New York Times Article

the smart cards tamper proof by drawing mathematical inferences from the fluctuating electrical power consumption of the chip. It is a sophisticated type of analysis, but the rudimentary "laboratory" -- in this case a three-room office suite, some garden-variety PC's and several thousand dollars of electronics equipment -- indicates that it does not require elaborate tools to crack what is supposed to be a highly secure digital safe.

As details of the technique circulate, as they invariably do in the hacker underground, imitators will almost certainly try to duplicate Kocher's experiment. For his part, Kocher, who at 25 is already a well-known expert in code breaking, said, "As the expertise becomes more widely available, the threats will become more than academic."

Peter Neumann, a computer scientist at SRI International, a research group in Menlo Park, Calif., said the approach had "enormous potential as another technique for breaking weakly designed and badly implemented devices."

Related Article
Cryptographers Discuss Finding Of Security Flaw in 'Smart Cards'
(June 10)

Though already in wide use as bank cards in Europe, smart cards in this country have been mainly used so far for controlling access to buildings and protecting against fraudulent use of new types of cellular telephones. But American banks have begun experimenting with the cards, as Chase Manhattan is doing in a test of Mastercard International's Mondex system on the Upper West Side of Manhattan.

Banks trust that the computer chips embedded in tamper-resistant packaging will act like a virtual branch office, dispensing money and crediting accounts to the right people.

But if someone could break through the card's defense, then that person could conduct fraudulent transactions, load counterfeit digital cash onto the cards or create various other forms of mischief.

So even as smart-card executives seek to play down the threat posed by Kocher's discovery, and they stress that no known break-ins of his sort have occurred in the real world, the industry knows it must continuously improve smart-card software and hardware.

"In a sense, this is an arms race; the attackers will always get better," said Richard Fletcher, the head of strategy and planning of Mastercard's Mondex smart-card division. "The only defense and the best defense against future attacks is to keep moving and keep changing."

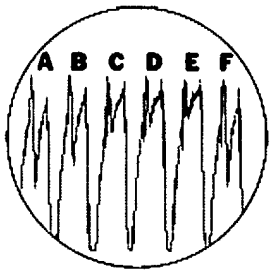
Gerald Hubbard is the vice president of marketing in the United States for Bull Smart Cards, a company that says it has shipped more than 120 million money-carrying smart cards

Cracking the Code

By monitoring the power consumption of smart cards, an expert in electronic security has discovered a way to crack the code that protects information on the cards -- credit-card size devices that contain a tiny computer chip and can be used for a variety of purposes,

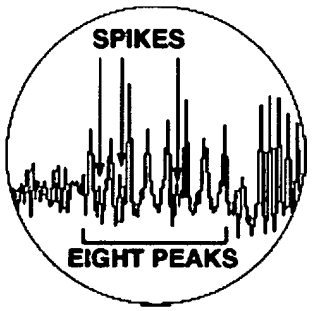
APPENDIX A
New York Times Article

including storing so-called digital cash. Here is how the security code can be breached.



Looking for Patterns

When the card is in use, its microchip performs a number of operations, each of which requires different amounts of power. By hooking the card up to an oscilloscope, a machine that records power use, the distinctive patterns from each operation can be recorded. Above are six operations done by a smart card in 1.68 microseconds. As recorded by the oscilloscope, operations A and F are identical, as are C and D. This series of peaks occurs whenever the card performs that series of operations. If one peak is omitted at some point, it would indicate an important change in the computation.



Doing More Analysis

Because looking at the pattern created by a number of computational cycles is not enough to figure out the security codes, other types of analysis are needed, like the example above. Each point on these peaks depicts an average of four cycles like the ones

throughout the world. He said that his company had known about the Kocher type of attack for more than four years and had installed safeguards to thwart it. But, Hubbard said, "You can never say a card is 100 percent immune."

In fact, some other industry executives expect it to take perhaps two years before there will be smart cards and related hardware that will be impervious to Kocher's type of attack. Kocher said he had approached the smart-card industry last year with the details of his discovery because he knew that criminals might also use the same tricks. But he said that he did not publicize his findings so that the industry would have time to adopt defenses, including techniques for which he has filed for patents and is now licensing to the companies.

He publicly announced the smart-card security flaw two weeks ago, only after The Australian Financial Review published an article about his break-in technique.

Kocher's company, Cryptography Research, analyzes and tests computer security hardware and software for many of the leading computer companies. His discoveries of flaws in supposedly secure technologies have drawn attention in the past -- as in 1995, when he found that he could break into smart cards by simply timing how long it took them to process data.

In the case of this newly disclosed smart-card problem, Kocher and his colleagues found that the cards' consumption of electrical power could disclose vital information about the secret key that protects the money or other data on the chip.

By watching the monitor of an oscilloscope, a device that measures the power use on a screen similar to the way a cardiac monitor displays a patient's heart action, Kocher's team was able in some cases to use the electrical pattern from a single transaction to decipher the key to the code. In other cases, they were forced to use more sophisticated statistical techniques to analyze the results from as many as 1,000

APPENDIX A
New York Times Article

above. The sequence of eight peaks indicates a part of an encryption operation that protects information on the card. The presence or absence of spikes between these peaks gives analysts a piece of the encryption key, of which further, similar analysis may reveal additional pieces.

transactions.

Kocher said his team had spent at least as much time looking for solutions as it had in identifying the security flaw. A possible remedy involves masking the transaction in digital noise by adding meaningless random calculations that would consume random amounts of current.

Another possible solution, which according to Mastercard officials is being incorporated in the latest version of its Mondex smart-card software, is to vary the order of the operations in the software to make it more difficult to identify patterns in the consumption of power.

A banking industry goal with smart cards is to cut costs by eliminating the need for central approval of a debit or credit transaction. By some estimates, the marginal costs for clearing a smart-card transaction are well under a penny.

Credit card transactions, however, typically require a long-distance computer network and a large central data base for examining each deal, and the transaction eventually means billing a customer and cashing the payment checks. These steps add up to 25 cents a transaction, on average, compared with about a penny for a smart-card transaction, in which all the authorization information -- and even the money itself -- can be contained on the card's chip.

To create an audit trail that might help track fraud, however, Visa International's smart-card system uses merchant terminals that report transactions to a central data base at the end of each day.

"We don't feel it is a good idea to have the security depend upon the chip itself," said Philip Yen, a senior vice president of Visa International. "We think it's more important to have complete system security."

Fletcher, of Mastercard's Mondex, contends that including any sort of central control runs counter to the purpose of a smart card -- giving customers the ability to use the money on a card just like cash.

"The critical point of any digital cash system is that you're off line," he said. "There's no online link at that point. You're critically dependent upon the card's security."

As the banks debate the security trade-offs, there is one certainty: Paul Kocher and others like him will continue to look for chinks in the smart-card armor. And as Kocher likes to remind the industry, "We have not yet encountered a card that couldn't be broken."

Related Sites

Following are links to the external Web sites mentioned in this article. These sites are not part of The New York Times on the Web, and The Times has no control over their content or

APPENDIX A
New York Times Article

availability. When you have finished visiting any of these sites, you will be able to return to this page by clicking on your Web browser's "Back" button or icon until this page reappears.

- Visa International Smart Cards
- Mastercard International Smart Cards
- Bull Smart Cards
- SRI International
- Chase Manhattan Bank
- Cryptography Research

Peter Wayner at wayner@nytimes.com welcomes your comments and suggestions.

APPENDIX A
New York Times Article